PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-007533

(43)Date of publication of application : 08.01.2004

(51)Int.Cl. H04N 5/92
G06F 12/14
G09C 1/00

(21)Application number : 2003-092358

(22)Date of filing : 28.03.2003

(71)Applicant : TOSHIBA CORP

(72)Inventor : SATO JUN
TERAUCHI TORU

(30)Priority

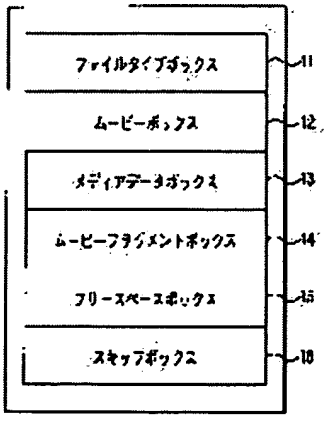
Priority number : 2002097757 Priority date : 29.03.2002 Priority country : JP

(54) DATA STRUCTURE OF MULTIMEDIA/FILE/FORMAT, METHOD AND DEVICE FOR DATA ENCRYPTION, AND METHOD AND DEVICE FOR DECRYPTING ENCRYPTED DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the data structure of multimedia/files/formats, which is allowed to efficiently access a prescribed position of contents data, an encrypting method for encrypting the data and a decrypting method for decrypting the encrypted data.

SOLUTION: In the data structure of multimedia/files/formats, a movie box and a media data box are prepared. Respective boxes are provided with non-encrypted sizes/fields, types/fields and boxes/data/fields. Information data concerned with non-encrypted or encrypted multimedia data are stored in the box/data/field of the movie box and encrypted multimedia/data are stored in the box data/field of the media data box.



LEGAL STATUS

[Date of request for examination]	28.03.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3748437
[Date of registration]	09.12.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

拒絶引用S04P1436W000

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-7533
(P2004-7533A)
(43)公開日　平成16年1月8日(2004.1.8)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04N	5/92	H04N	5/92	H	5B017
G06F	12/14	G06F	12/14	320B	5C053
G09C	1/00	G09C	1/00	660D	5J104

審査請求 有　請求項の数 18　OL　（全 22 頁）

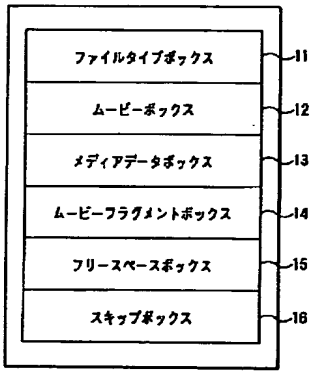
(21)出願番号　特願2003-92358(P2003-92358)
(22)出願日　平成15年3月28日(2003.3.28)
(31)優先権主張番号　特願2002-97757(P2002-97757)
(32)優先日　平成14年3月29日(2002.3.29)
(33)優先権主張国　日本国(JP)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目1番1号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】マルチメディア・ファイル・フォーマットのデータ構造、その暗号化方法並びに装置及びその暗号の復号化方法及び装置

(57)【要約】
【課題】コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法を提供するにある。
【解決手段】マルチメディア・ファイル・フォーマットのデータ構造においては、ムービーボックス及びメディアデータボックスが設けられている。各ボックスは、非暗号化されたサイズ・フィールド及びタイプ・フィールド並びにボックス・データ・フィールドを備えている。ムービーボックスのボックス・データ・フィールドには、非暗号化或いは暗号化されたマルチメディア・データに関する情報データが格納され、メディアデータボックスのボックス・データ・フィールドには、暗号化されたマルチメディア・データが格納されている。
【選択図】　図1



【特許請求の範囲】
【請求項１】
当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び
当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、
から構成されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造。
【請求項２】
前記第１或いは第２のボックスは、前記第１及び第２のサイズ・フィールドが夫々所定の値を有するとき、夫々当該サイズ・フィールドと共に当該ボックスのサイズをバイトで示すための第１及び第２のロングサイズ・フィールド含むことを特徴とする請求項１のマルチメディア・ファイル・フォーマットのデータ構造。
【請求項３】
前記第１のボックスでは、前記マルチメディア・データの音声或いは動画の符号化データがサンプル列として第１のボックス・データ・フィールドに格納され、当該サンプルは、暗号化符号化データを含むことを特徴とする請求項１のマルチメディア・ファイル・フォーマットのデータ構造。
【請求項４】
前記第１のボックスでは、前記マルチメディア・データの音声或いは動画の符号化データがサンプル列として第１のボックス・データ・フィールドに格納され、１又は複数のサンプルがチャンクに定められ、当該チャンクは、暗号化符号化データを含むことを特徴とする請求項１のマルチメディア・ファイル・フォーマットのデータ構造。
【請求項５】
前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャンク、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項３又は請求項４のいずれかに記載のマルチメディア・ファイル・フォーマットのデータ構造。
【請求項６】
前記情報データが暗号化されて第２のボックス・データ・フィールドに格納されることを特徴とする請求項１のマルチメディア・ファイル・フォーマットのデータ構造。
【請求項７】
第１のサイズ・フィールド、第１のタイプ・フィールド及び第１のボックス・データ・フィールドを含む第１のボックスと、及び第２のサイズ・フィールド、第２のタイプ・フィールド及び第２のボックス・データ・フィールドを有する第２のボックスとから構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する方法において、
前記マルチメディア・データを暗号化して第１のボックス・データ・フィールドに格納し、
前記第１のボックス・データ・フィールドに格納されたマルチメディア・データに関する情報データを第２のボックス・データ・フィールドに格納し、
夫々前記第１及び第２のボックスのサイズをバイトで示すための第１及び第２のサイズ情報を暗号化せずに前記第１及び第２のサイズ・フィールドに格納し、及び
夫々前記第１及び第２ののボックスの種別を識別する第１及び第２のタイプ情報を記述する前記第１及び第２のタイプ・フィールドを暗号化せずに第１及び第２のボックスに格納

することを特徴とする暗号化方法。
【請求項８】
前記マルチメディア・データの音声或いは動画の符号化データがデータ単位としてのサンプル列に分離され、このデータサンプルが暗号化されて前記第１のボックス・データ・フィールドに格納されていることを特徴とする請求項７の暗号化方法。
【請求項９】
前記マルチメディア・データの音声或いは動画の符号化データがデータ単位としてのサンプル列に分離され、１又は複数のサンプルがチャンクに定められ、このチャンクが暗号化されて前記第１のボックス・データ・フィールドに格納されていることを特徴とする請求項７の暗号化方法。
【請求項１０】
前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャンク、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項８又は請求項９のいずれかに記載の暗号化方法。
【請求項１１】
前記情報データは暗号化されて第２のボックス・データ・フィールドに格納されることを特徴とする請求項７に記載の暗号化方法。
【請求項１２】
第１のサイズ・フィールド、第１のタイプ・フィールド及び第１のボックス・データ・フィールドを含む第１のボックスと、及び、第２のサイズ・フィールド、第２のタイプ・フィールド及び第２のボックス・データ・フィールドを有する第２のボックスと、から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する装置であって、
前記マルチメディア・データを暗号化して第１のボックス・データ・フィールドに格納する暗号化部と、
前記マルチメディア・データに関する情報データを第２のボックス・データ・フィールドに格納する第１の格納部と、
夫々第１及び第２のサイズ情報を暗号化せずに前記第１及び第２のサイズ・フィールドに格納する第２の格納部と、及び
前記第１及び第２のボックスの種別を識別する第１及び第２のタイプ・フィールドを夫々暗号化せずに対応するボックスに格納する第３の格納部と、
から構成されることを特徴とする暗号化装置。
【請求項１３】
前記暗号化部は、マルチメディア・データの音声或いは動画の符号化データをデータ単位としてのサンプル列に分離し、このデータサンプルを暗号化して前記第１のボックス・データ・フィールドに格納することを特徴とする請求項１２の暗号化装置。
【請求項１４】
前記暗号化部は、前記マルチメディア・データの音声或いは動画の符号化データをデータ単位としてのサンプル列に分離し、１又は複数のサンプルをチャンクに定め、このチャンクを暗号化されて前記第１のボックス・データ・フィールドに格納することを特徴とする請求項１２の暗号化装置。
【請求項１５】
前記暗号化部において、前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャンク、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項１３又は請求項１４のいずれかに記載の暗号化装置。
【請求項１６】
第１の格納部は、前記情報データを暗号化して第２のボックス・データ・フィールドに格納することを特徴とする請求項１２に記載の暗号化装置。

【請求項１７】
当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び
当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、
から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する方法において、
前記第２のボックスデータに格納されている情報データを獲得してこれを保持し、及び
この情報データを基にして前記第１のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力することを特徴とする暗号復号化方法。
【請求項１８】
当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び
当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、
から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する装置において、
前記２のボックスデータに格納されている情報データを獲得してこれを保持する獲得部と、及び
この情報データを基にして前記第１のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力する出力部と、
を具備することを特徴とする暗号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、マルチメディア・ファイル・フォーマットのデータ構造、その暗号化方法並びに装置及びその暗号の復号化方法及び装置に係り、特に、動画記録装置及び再生装置における動画ファイルの暗号化方法及びその装置に関する。
【０００２】
【従来の技術】
近年、動画などのコンテンツは、アナログ・データからデジタル・データに移行しつつある。デジタル化されたコンテンツは、品質の劣化無しにコピーできるため、ユーザ間でＣＤ－Ｒ、記録可能ＤＶＤディスク、或いは、メモリーカードを介して、又は、インターネット等の通信手段を利用したファイル転送技術、例えば、Ｅメールに添付してコンテンツ・データを送ってコンテンツ・データをコピーすることが可能となり、このようなコピーが横行しつつあり、コンテンツ業界で著作権上問題となっている。
【０００３】
デジタルコンテンツの著作権を保護するための解決手段として、コンテンツデータに暗号をかける方法があり、この暗号化によってて不正なコピーを防ぐことができる。従来のコンテンツデータに暗号をかける場合、一般にコンテンツデータの先頭から終端まで一括し

て暗号化する方法がとられている。これにより、コンテンツデータを利用する権利があるもの、即ち、暗号を解く権限があり、その手段を有するもののみがコンテンツデータを利用することが可能となる。

【０００４】

【発明が解決しようとする課題】

上述したような従来の暗号化方法においては、コンテンツデータを先頭から終端まで一括して暗号化する場合には、コンテンツデータの不正コピーを防ぐことはできる。しかしながら、コンテンツデータの先頭から終端まで一括して暗号化しているため、コンテンツデータの任意の位置にアクセスすることが容易でなく、任意の位置にアクセスする為には、アクセス対象とされていないデータであっても復号化して暗号化を解く必要があり、実質上、無駄な処理が要求される問題がある。即ち、従来、暗号化されたコンテンツデータの任意の位置にアクセスする際には、コンテンツの先頭から順次暗号を解き、所望のコンテンツの位置に到達するまで暗号を解く処理が必要とされる。このような処理は、アクセス位置のデータを獲得するまでに処理時間が係る問題がある。

【０００５】

このように所望のコンテンツの位置に到達するまでの暗号を解く処理は、所望の位置をアクセスするためのみに必要とされる処理であって、実際にコンテンツデータを利用するために必要とされる処理ではないことから、無駄な処理ということができる。

【０００６】

所望するアクセス位置がファイルの先頭から離れれば離れるほど、上記の無駄な処理及び処理時間は増大する。処理負荷及び処理時間が増大するとそれに伴い消費電力も増大することになるので、バッテリを利用するポータブル機器などには連続使用時間が削減されるという問題もある。

【０００７】

コンテンツデータの任意の位置へのアクセスは、動画の再生においては、例えば、早送り再生、巻き戻し再生、ランダムアクセス再生、レジューム再生（ユーザが再生停止したところから、再度再生を再開する機能）を実現するときに必要とされる。

【０００８】

この発明は、上述した事情に鑑みなされたものであって、その目的は、コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法を提供するにある。

【０００９】

【課題を解決するための手段】

この発明によれば、

当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び

当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、

から構成されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造が提供される。

【００１０】

また、この発明によれば、

第１のサイズ・フィールド、第１のタイプ・フィールド及び第１のボックス・データ・フィールドを含む第１のボックスと、及び第２のサイズ・フィールド、第２のタイプ・フィールド及び第２のボックス・データ・フィールドを有する第２のボックスとから構成され

るファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する方法において、
前記マルチメディア・データを暗号化して第１のボックス・データ・フィールドに格納し、
前記第１のボックス・データ・フィールドに格納されたマルチメディア・データに関する情報データを第２のボックス・データ・フィールドに格納し、
夫々前記第１及び第２のボックスのサイズをバイトで示すための第１及び第２のサイズ情報を暗号化せずに前記第１及び第２のサイズ・フィールドに格納し、及び
夫々前記第１及び第２ののボックスの種別を識別する第１及び第２のタイプ情報を記述する前記第１及び第２のタイプ・フィールドを暗号化せずに第１及び第２のボックスに格納することを特徴とする暗号化方法が提供される。

【００１１】
更に、この発明によれば、
第１のサイズ・フィールド、第１のタイプ・フィールド及び第１のボックス・データ・フィールドを含む第１のボックスと、及び、第２のサイズ・フィールド、第２のタイプ・フィールド及び第２のボックス・データ・フィールドを有する第２のボックスと、から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する装置であって、
前記マルチメディア・データを暗号化して第１のボックス・データ・フィールドに格納する暗号化部と、
前記マルチメディア・データに関する情報データを第２のボックス・データ・フィールドに格納する第１の格納部と、
夫々第１及び第２のサイズ情報を暗号化せずに前記第１及び第２のサイズ・フィールドに格納する第２の格納部と、及び
前記第１及び第２のボックスの種別を識別する第１及び第２のタイプ・フィールドを夫々暗号化せずに対応するボックスに格納する第３の格納部と、
から構成されることを特徴とする暗号化装置が提供される。

【００１２】
更にまた、この発明によれば、
当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び
当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、
から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する方法において、
前記第２のボックスデータに格納されている情報データを獲得してこれを保持し、及び
この情報データを基にして前記第１のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力することを特徴とする暗号復号化方法が提供される。

【００１３】
また更に、この発明によれば、
当該第１のボックスのサイズをバイトで示すための第１の非暗号化サイズ情報を格納する第１のサイズ・フィールド、当該第１のボックスの種別を識別する第１の非暗号化タイプ情報を格納する第１のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第１のボックス・データ・フィールドを含む第１のボックスと、及び

当該第２のボックスのサイズをバイトで示すための第２の非暗号化サイズ情報を格納する第２のサイズ・フィールド、当該第２のボックスの種別を識別する第２の非暗号化タイプ情報を格納する第２のタイプ・フィールド及び前記第２のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第２のボックス・データ・フィールドを含む第２のボックスと、
から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する装置において、
前記２のボックスデータに格納されている情報データを獲得してこれを保持する獲得部と、及び
この情報データを基にして前記第１のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力する出力部と、
を具備することを特徴とする暗号化装置が提供される。

【００１４】

【発明の実施の形態】

以下、図面を参照しながらこの発明の暗号化方法の一実施例について説明する。

【００１５】

この発明の暗号化方法がＭＰＥＧ－４ファイル・フォーマットに適用される実施例について図１から図１８を参照して説明する。

【００１６】

図１は、ＩＳＯにて規格化されているＭＰＥＧ－４ファイル・フォーマット（ＦＩＬＥ ＦＯＲＭＡＴ）の構造を示している。以下の説明において、ＭＰＥＧ－４ファイル・フォーマットは、単にＭＰ４と省略して説明する。ＭＰ４は、ＭＰＥＧ－４に従って符号化されたビデオストリーム、或いは、オーディオストリームを格納するためのファイル・フォーマットである。このファイル・フォーマットには、定義により、ＭＰＥＧ－４以外のコーデックも格納することが可能である。尚、このＭＰ４データは、ファイルとしてディスク上に格納されている場合、或いは、バイナリイメージとしてメモリ上に格納されている場合等が想定される。

【００１７】

図１に示すように、ＭＰ４は、オブジェクト構造を有し、幾つかのボックスより構成されている。このボックスは、文献によりアトム（ａｔｏｍ）と称せられる場合があることに注意されたい。ＭＰ４では、ボックス中に、さらにボックスを入れた入れ子状態で格納することができるとされている。ここで、入れ子状態、即ち、階層構造になっているボックスの最初のボックス、即ち、最上位のボックスは、トップレベルボックスと称せられる。図１には、トップレベルボックスのみが示されている。

【００１８】

図１に示すように、トップレベルボックスは、幾つかの種類がある。即ち、ＭＰ４ファイルは、ファイルタイプボックス１１、ムービーボックス１２、メディアデータボックス１３、ムービーフラグメントボックス１４、フリースペースボックス１５及びスキップボックス１６等から構成される。これらのボックスは、ＭＰ４ファイル中に必須のもの、或いは、オプションで記述されれば良いものがある。

【００１９】

ＭＰ４では、これらのボックスは、図１に示すような順序で配列されることは要求されず、前述したような規定項目の範囲内で構成を変更することが可能である。しかし、ここでは、特に具体的な規定内容については説明を省略する。ただし、ボックスによって出現個数、位置、有無が規定され、データによりトップレベルボックスの構成が異なることがＭＰ４の特徴であるとされている。

【００２０】

ここで、各トップレベルボックスの機能について説明する。ファイルタイプボックス１１は、ファイルのブランド或いはバージョン等のファイルのタイプを格納するボックスであり、ＭＰ４で定まったファイルであることを記述している。ムービーボックス１２は、Ｍ

Ｐ４データ全体のメタデータ、つまり符号化されたメディアのコーデックストリームをデコードするために必要な情報等、例えば、データのデコードに必要とされる属性及びアドレス等が記述されている情報を格納している。メディアデータボックス１３は、実際の符号化されたメディアのコーデックストリーム、即ち、ビデオストリーム、或いは、オーディオストリーム等のコンテンツデータを格納している。ムービーフラグメントボックス１４は、ムービーボックス１２の情報を分割して格納するためのボックスである。フリースペースボックス１５及びスキップボックス１６は、ユーザーデータや、パディングのためにパディングデータを格納するためのボックスである。ユーザデータボックス１７は、ユーザが定めたデータが格納されるボックスである。

【００２１】

次に、ボックスの構造について説明する。ボックスは、全てのボックスにおいて共通の構造を有している。図２には、共通の構造を有するボックス２０を示している。このボックス２０においては、先頭の４バイトがボックスのサイズをバイトで示すためのサイズ・フィールド２１に定められている。次の、４バイトは、ボックスの種別を識別するタイプ・フィールド２２に定められている。ボックスの種別は、４つのキャラクターにより識別され、例えば、ムービーボックス１２の場合は‘ｍｏｏｖ’となり、ムービーデータボックスの場合は‘ｍｄａｔ’となる。この４文字のキャラクターをマッチングさせることによりボックスの種別を識別することが可能となる。次に、タイプ・フィールド２２に続いてボックス・データ・フィールド２３が格納されている。このボックス・データ・フィールドの構造は、各ボックスにおいて用途によりシンタックスが定義されている。このボックス・データ・フィールドのサイズは、サイズ・フィールド２１の値からサイズ・フィールド２１とタイプ・フィールド２２で用いられている８を除いた値となる。

【００２２】

図３に示すように、サイズ・フィールドの値が１のときは（Ｓｉｚｅ＝＝１）、このボックス２０では、タイプ・フィールド２２とボックス・データ・フィールド２３の間に当該サイズ・フィールド２４とともにボックスのサイズを示す８バイトのラージサイズ・フィールド２４が出現し、ボックスのサイズが４バイトのサイズ・フィールド２１で表現できないような大容量のボックスにも対応できるようになっている。このボックス２０では、ボックス・データ・フィールド２３のサイズは、ラージサイズ・フィールドに格納されているサイズから１６を除いた値となる。

【００２３】

この発明の一実施例に係る暗号化方法においては、トップレベルのボックス毎にデータが暗号化及び非暗号化が決定される。即ち、図４に示すようにサイズ・フィールド２４の値が１でない場合（ｓｉｚｅ！＝１）のサイズ・フィールド及びタイプ・フィールドのデータは、暗号化されず（以下、単に暗号化されていない場合は、非暗号化と称する場合がある。）、ボックスデータが暗号化の対象とされている。

【００２４】

尚、メディアデータボックス１３のメディアデータは、後に述べるように暗号化されることが必須とされる。他のボックス１１、１２、１４～１６のボックスデータは、後に述べるように暗号化されても良く或いはされなくとも良い。

【００２５】

図５に示されるように、サイズ・フィールド２４の値が１で、タイプ・フィールド２２とボックスデータ部２３の間にラージサイズ・フィールド２４がある場合にあっても、このラージサイズ・フィールド２４も暗号化の対象とされない。暗号化の方法によっては、データのブロック長が複数バイト必要な場合がある。即ち、暗号化の対象とされるデータが所定のブロック長で分割されてデータが暗号化される場合には、所定のブロック長未満の残余のデータが生じ、このデータ長が暗号化に必要とされるバイト数に達しない虞がある。このように暗号化されるデータ中で残余のバイトが生じ、このバイト数が暗号化の対象バイト数よりも小さい場合には、図６に示されるように、この残余のブロック中の残余のデータに対しては、暗号化しないようにしても良い。一例としては、ボックスデータ長が

１５バイトで、暗号手法がデータのブロック長を８バイト必要とする場合が該当する。この場合、ボックスデータの最初の８バイトは、暗号化され、残りの７バイトは暗号化されないこととなる。

【００２６】

以上のように、ボックスデータ部に対してデータを暗号化することで、例えば、ムービーボックス１２にアクセスが試みられた際に、始めに、ＭＰ４データの先頭の８バイトが取得されてボックスサイズ及びボックスタイプ・フィールドが獲得される。次に、ボックスタイプがムービーボックス１２のタイプと一致するかが確認される。一致しない場合、即ち、ボックスタイプがムービーボックス１２のタイプでない場合には、アクセスポインタがボックスサイズ分だけずらされ、次の８バイトが取得されてボックスサイズとボックスタイプ・フィールドが獲得される。ボックスタイプがムービーボックス１２のタイプと一致するまでこのアクセスポインタのシフトが繰り返えされる。ボックスタイプがムービーボックス１２のタイプと一致すると、暗号化されているボックスデータは、順次その暗号化が解れてムービーボックス１２中のボックスデータへアクセスすることが可能となる。

【００２７】

次に、メディアデータボックス１３中のメディアデータは、暗号化される場合について説明する。

【００２８】

メディアデータボックス１３は、他のトップレベルボックスがメディアストリームのデコードに必要な情報を格納しているのと異なり、メディアデータが格納されている。このメディアデータの暗号化に際しては、スキップ再生、早送り再生、巻き戻し再生、或いは、レジューム再生等の特殊再生時に、メディアデータの任意の位置に効率よくアクセスすることができることが必要とされる。そのために、図６に示すように、上述のサイズ・フィールド及びタイプ・フィールドを暗号化しないことに加え、ストリームデータは、独立した符号化単位毎に暗号化がなされる。ここでは、符号化単位とは、音声ストリームに関しては、サンプル、若しくは、フレームが相当し、動画ストリームに関しては、フレームが相当する。

【００２９】

この発明に実施例に係るメディアデータボックス１３内のメディアデータの暗号化では、暗号化される符号化の単位は、ＭＰ４データ内のサンプルが対象とされる。サンプルに代えて、チャンクがメディアデータボックス１３内で暗号化されても良い。各サンプルについてのＭＰ４データ内での位置は、そのサンプルについて記述するムービーボックス１２のチャンクオフセット及びサンプルサイズを解析することによって得ることができる。即ち、サンプルが属するチャンクの位置は、データファイル先頭からのオフセットとしてチャンクオフセットに記述され、そのチャンクに含まれるサンプルについては、そのサイズがサンプルサイズに記述されている。従って、何れのサンプルもチャンクオフセット及びサンプルサイズを参照することによって、そのオフセットを求めることができる。

【００３０】

ここで、より説明を明確にする為にＭＰ４におけるムービーボックス１２の構造及びメディアデータボックス１３内のデータ構造を図８から図１０を参照して説明する。

【００３１】

図８は、ｍｏｏｖ（Ｍｏｖｉｅ　Ｂｏｘ）と称せられるムービーボックス１２の構造を示している。この図８に示されるボックスには、図４から図８を参照して説明した暗号化の対象とされないサイズ・フィールド、ラージサイズ・フィールド及びタイプ・フィールドは、図示されず、データボックス部に相当するムービーボックス１２（ムービーボックス：Ｍｏｖｉｅ　Ｂｏｘ）のみが示されている。同様に図８には、メディアデータボックス１３としてｍｄａｔ（メディアデータボックス１３：Ｍｅｄｉａ　Ｄａｔａ　Ｂｏｘ）が示されているが、この内には、サイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドがあり、ボックスデータとして実データとしてのコンテンツデータ（マルチメディア・データ）が格納されている。図８及び図９Ａ及び９Ｂを参照する

説明においては、サイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドがあるものとして説明を理解されたい。

【００３２】

この図８に示されるフォーマットでは、１つのＭＰ４ファイルは、第１階層のヘッダとしてファイル情報が記載されるｍｏｏｖ（ムービーボックス：Ｍｏｖｉｅ　Ｂｏｘ）及び音声データ及び映像データを含むマルチメディア・データが格納されているｍｄａｔ（メディアデータボックス１３：Ｍｅｄｉａ　Ｄａｔａ　Ｂｏｘ）から構成されている。このＭＰ４ファイルには、付加的に、第１階層の空き領域としてのｆｒｅｅ（フリー）並びにｓｋｉｐ（スキップ）及びユーザが定義する書き込みを許すｕｄｔａ　（ユーザデータボックス：Ｕｓｅｒ　Ｄａｔａ　Ｂｏｘ）が設けられている。

【００３３】

尚、ＭＰ４ファイルでは、一般にボックス（ｂｏｘ）と称される単位を元にデータを分類し、管理されている。このボックス（ｂｏｘ）は、上位層から下位層に至る階層構造を取ることができ、その内部に更に下位層のボックス（ｂｏｘ）を含むものを「コンテナボックス」と称している。ここで説明するボックスは、アトム（ａｔｏｍ）と称される場合がある。

【００３４】

また、ヘッダとしてのｍｏｏｖ（Ｍｏｖｉｅ　Ｂｏｘ）には、第２階層にあるＭＰ４ファイルの作成時刻及びＭＰ４ファイルのコンテンツ長等のヘッダ情報が記述されているｍｖｈｄ　（ムービーヘッダボックス：Ｍｏｖｉｅ　Ｈｅａｄｅｒ　Ｂｏｘ）、オブジェクト、即ち、再生対象に関する情報が記述されているｉｏｄｓ（オブジェクトディスクリプタボックス：Ｏｂｊｅｃｔ　ｄｅｓｃｒｉｐｔｏｒ　Ｂｏｘ）及び多重化されているメディア情報に関する各種パラメータが記述されているｔｒａｋ　（トラック：Ｔｒａｃｋ　Ｂｏｘ）を含んでいる。このｔｒａｋ　（Ｔｒａｃｋ　Ｂｏｘ）は、多重化されているメディアが多数あれば、そのメディアの数だけ用意される。例えば、音声と映像とが多重化されたコンテンツにあっては、音声メディアトラック及び映像メディアのトラックが用意され、その音声用のトラックに音声メディアのパラメータが格納され、映像用のトラックに映像メディアのパラメータが格納される。

【００３５】

図８に示されるようにトラック（Ｔｒａｃｋ　Ｂｏｘ）は、第３階層にあるトラックの作成時刻及びトラックＩＤ（識別子）と称されるトラックを識別するための一連の番号が格納されているｔｋｈｄ　（トラックヘッダボックス：Ｔｒａｃｋ　Ｈｅａｄｅｒ　Ｂｏｘ）、トラックに関して記述されたｔｒｅｆ　（トラックリファレンスボックス：Ｔｒａｃｋ　Ｒｅｆｅｒｅｎｃｅ　Ｂｏｘ）、編集情報に関してのｅｄｔｓ　（エデットボックス：Ｅｄｉｔ　Ｂｏｘ）及びメディアの情報に関して記述されたｍｄｉａ　（メディアボックス：Ｍｅｄｉａ　Ｂｏｘ）を含んでいる。エデットボックスｅｄｔｓは、第４階層に編集リスト情報が記述されたｅｌｓｔ　（エデットリスト：ボックスＥｄｉｔ　Ｌｉｓｔ　Ｂｏｘ）を含み、メディアボックスｍｄｉａは、第４階層にこのメディアトラックのタイムスケール等の情報が格納されるｍｄｈｄ（メディアヘッダ：Ｍｅｄｉａ　Ｈｅａｄｅｒ）、ヘッダを参照する情報が記述されたｈｄｌｒ（ヘッダリファレンスボックス：Ｈａｎｄｌｅｒ　Ｒｅｆｅｒｅｎｃｅ　Ｂｏｘ）及びメディアに関する情報が格納されているｍｉｎｆ（メディアインフォメーションボックス：Ｍｅｄｉａ　ｉｎｆｏｒｍａｔｉｏｎ　Ｂｏｘ）を含んでいる。メディアインフォメーションｍｉｎｆは、更に第５階層にトラックに格納されているメディアが映像であることを示すｖｍｈｄ（ビデオメディアヘッダボックス：Ｖｉｄｅｏ　Ｍｅｄｉａ　Ｈｅａｄｅｒ　Ｂｏｘ）、或いは、トラックに格納されているメディアが音声であることを示すｓｍｈｄ　（サウンドメディアヘッダボックス：Ｓｏｕｎｄ　Ｍｅｄｉａ　Ｈｅａｄｅｒ　Ｂｏｘ）、ヒント・メディアのヘッダ情報が記述されたｈｍｈｄ（ヒントメディアヘッダボックス：Ｈｉｎｔ　Ｍｅｄｉａ　Ｈｅａｄｅｒ　Ｂｏｘ）、メディアがビデオ或いは音声以外のＭＰＥＧ－４ストリームである場合に、ＭＰＥＧ－４のヘッダ情報が記述されたｍｐｅｇ（ＭＰＥＧ－４メディアボックス：

ＭＰＥＧ－４　Ｍｅｄｉａ　Ｂｏｘ）、メディア情報が記述されたｍｉｎｆ（メディアインフォメーションボックス：Ｍｅｄｉａ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂｏｘ）及びサンプルに関しての情報が記述されたｓｔｂｌ（サンプルテーブルボックス：ＳａｍｐｌｅＴａｂｌｅ　Ｂｏｘ）を含んでいる。ビデオメディアヘッダボックスｖｍｈｄ及びサウンドメディアヘッダボックスｓｍｈｄは、トラックに格納されているメディア、即ち、音声か映像化の種別に応じて択一的に記載される。更にまた、ｄｉｎｆ（データインフォメーションボックス：Ｄａｔａ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂｏｘ）は、データを参照する情報が記述されたｄｒｅｆ（データリファレンスボックス：Ｄａｔａ　Ｒｅｆｅｒｅｎｃｅ　Ｂｏｘ）を含み、また、ｓｔｂｌ（サンプルテーブルボックス：Ｓａｍｐｌｅ　Ｔａｂｌｅ　Ｂｏｘ）は、各サンプルのデコード時刻が設定されているｓｔｔｓ（デコーディングタイム：Ｄｅｃｏｄｉｎｇ　ｔｉｍｅ　ｔｏ　Ｓａｍｐｌｅ　Ｂｏｘ）、サンプルに対する表示．時間が記述されたｃｔｔｓ　（コンポジションタイム：Ｃｏｍｐｏｓｉｔｉｏｎ　Ｔｉｍｅ　ｔｏ　Ｓａｍｐｌｅ　Ｂｏｘ）、サンプルの同期情報が記述されたｓｔｓｓ（シンクロサンプルボックス：Ｓｙｎｃ　Ｓａｍｐｌｅ　Ｂｏｘ）、コーディックの種別やデコードに必要となる各種情報が設定されているｓｔｓｄ（サンプルディスクリプションボックス：Ｓａｍｐｌｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｂｏｘ）、トラック中のサンプルの総数（サンプルカウント：ｓａｍｐｌｅ＿ｃｏｕｎｔ）及び各サンプルのデータサイズ（エントリーサイズ：ｅｎｔｒｙ＿ｓｉｚｅ）が設定されているｓｔｓｚ（サンプルサイズボックス：Ｓａｍｐｌｅ　Ｓｉｚｅ　Ｂｏｘ）、チャンク内のサンプル数（チャンクに対するサンプル：ｓａｍｐｌｅ＿ｐｅｒ＿ｃｈｕｎｋ）及びサンプルのインデックス（サンプルディスクリプションインデックス：ｓａｍｐｌｅ＿ｄｅｓｃｒｉｐｔｉｏｎ＿ｉｎｄｅｘ）が記述されたｓｔｓｃ（チャンクに対するサンプル：Ｓａｍｐｌｅ　ｔｏ　Ｃｈｕｎｋ　Ｂｏｘ）、チャンクに関するファイルの先頭からのオフセット位置情報（チャンクオフセット：ｃｈｕｎｋ＿ｏｆｆｓｅｔ）が記述されるｓｔｃｏ　（チャンクオフセットボックス：Ｃｈｕｎｋ　Ｏｆｆｓｅｔ　Ｂｏｘ）、同期情報が記述されたｓｔｓｈ（シャドウシンクサンプルボックス：Ｓｈａｄｏｗ　Ｓｙｎｃ　Ｓａｍｐｌｅ　Ｂｏｘ）及びｓｔｄｐ（デグラデーションプライオリティボックス：ＤｅｇｒａｄａｔｉｏｎＰｒｉｏｒｉｔｙ　Ｂｏｘ）を含んでいる。ｓｔｓｄ（Ｓａｍｐｌｅ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｂｏｘ）は、必要に応じて複数個設定することができる。

【００３６】

ここで、図１０に示すようにサンプル（即ち、ｓａｍｐｌｅ）とは、映像や音声の実際のメディアデータをある大きさに区切った単位を称し、メディアデータは、このサンプルを基に管理されている。チャンク（即ち、ｃｈｕｎｋ）は、１又は複数のサンプルが連接されているものを称し、ファイル先頭からのチャンクの位置や当該チャンクにいくつのサンプルが含まれているかと言った、データ領域の内部構造に関する情報は、上述したようにｍｏｏｖコンテナボックスの下位階層に記述される。また、既に説明したように実際のメディアデータは、ｍｄａｔボックスに配置され、音声や映像といったメディア毎の情報管理にトラックというボックスが割り当てられている。このようにＭＰ４ファイルは、ｍｏｏｖコンテナボックスを取得すれば、構成されるメディア数、それぞれの種別、データサイズ等が判明する。

【００３７】

尚、一般にＭＰ４のボックスは、同一階層の配置順序の規定がない。図８の第１階層においては、ｍｏｏｖ、ｍｄａｔ、ｍｏｏｆ、ｆｒｅｅ、ｓｋｉｐ、ｕｄｔａの順序で並んでいるが、これは必ずしも規格上ファイル先頭からこの順番で並ばなければならないことを意味していない。例えば、図９Ａに示すようにｍｄａｔ、ｍｏｏｖ、ｆｒｅｅ、ｓｋｉｐ、ｕｄｔａの順序で並んでも良く、或いは、図９Ｂに示すようにｍｏｏｖ、ｕｄｔａ、ｍｄａｔ、ｍｏｏｆ、ｍｄａｔ、ｓｋｉｐ、ｆｒｅｅの順序で並んでも良い。更に、ＭＰ４ファイルでは、１つのｍｏｏｖに対して複数のｍｄａｔ、ｍｏｏｆが設けられても良い。

【００３８】

図８に示したサイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フ

ィールドを除くｍｏｏｖコンテナボックス内のデータ暗号化され、また、同様にサイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドを除くｍｄａｔコンテナボックス内の実データが暗号化される。

【００３９】

この暗号化は、一例として図１１に示すような動画像記録システム１００で実現され、この動画像記録システム１００において、音声及び映像データが図１２に示すような手順で暗号化される。この動画像記録システム１００における暗号化を含むフォーマットの手順についてこの図１１及び図１２を参照して説明する。

【００４０】

マイク１０１或いはオーディオ入力装置から取り込まれたオーディオ信号は、オーディオエンコーダ１０２でエンコードされて符号化オーディオデータ、例えば、ＭＰ４オーディオデータに変換される。同様に、カメラ１０３或いは映像入力装置から取り込まれたオーディオ信号は、ビデオエンコーダ１０４でエンコードされて符号化ビデオデータ、例えば、ＭＰ４ビデオデータに変換される。ここで、外部入力装置としてのマイク１０１、カメラ１０３からは、アナログ信号でも、或いは、デジタル信号の何れで動画像記録システム１００に入力されても良い。オーディオエンコーダ１０２からは、その内で生成された音声符号化ストリームがファイル生成部１０５へ出力され、ビデオエンコーダ１０４からは、同様に、その内で生成されたビデオ符号化ストリームがファイル生成部１０５へ出力される。ファイル生成部１０５では、オーディオエンコーダ１０２及びビデオエンコーダ１０４から出力された音声符号化ストリーム及びビデオ符号化ストリームが図８に示すような所定のＭＰ４ファイル・フォーマット形式に整えられ、ローカルメモリ１０６上に展開される。このファイル生成の完了後、図１２及び図１３を参照して説明するように暗号化部１０７がローカルメモリ１０６に蓄積されているファイルを所定の暗号化方法で暗号化し、再度ローカルメモリ１０６に配置し、暗号化ファイルとして出力する。

【００４１】

暗号化が開始されると（ステップＳ１０）、ステップＳ１１に示されるようにローカルメモリ１０６上へ展開されたＭＰ４ファイルからムービーボックス１２（ｍｏｏｖ）が検索される。ここで、ムービーボックス１２は、トップレベルボックスであるので、ファイルの先頭からサイズ・フィールド及びタイプ・フィールドを読み出し、タイプ・フィールドがｍｏｏｖと示されているものが捜される。最初のボックスがｍｏｏｖではない場合には、読み出したサイズ分だけファイル中でシークされ、次のボックスが解析される。タイプ・フィールドがｍｏｏｖとの表示があるまで検索が継続される。

【００４２】

ムービーボックス１２が検出されると、ムービーボックス１２中に格納されているトラック毎のチャンクオフセットボックス（ｓｔｃｏ）及びサンプルトゥチャンクボックス（ｓｔｓｃ）、サンプルサイズボックス（ｓｔｓｚ）が検索され、それらに保持されているテーブルがメモリ上に保持される。即ち、ステップＳ１２において、Ｎの初期値は１に設定され、このムービーボックス１２内の最初のトラックｔｒａｋ内に記述された最初のチャンクのチャンクオフセットｓｔｃｏが読み出され、このチャンクオフセットｓｔｃｏ内のｃｈｕｎｋ＿ｏｆｆｓｅｔからそのオフセットアドレスが読み出されると共にサンプルサイズボックスｓｔｓｚのｅｎｔｒｙ＿ｓｉｚｅからそのトラックに属する全てのサンプルサイズが読み出される。また、チャンクオフセットｓｔｃｏ内のｅｎｔｒｙ＿ｃｏｕｎｔからそのトラック内の全てのチャンク数が読み出され、また、チャンクボックスに対するサンプルを意味するｓｔｓｃのｓａｍｐｌｅ＿ｐｅｒ＿ｃｈｕｎｋから各チャンクのサンプル数が読み出され、サンプルサイズボックスｓｔｓｚのｓａｍｐｌｅ＿ｃｏｕｎｔからそのトラック内の全てのサンプル総数が読み出される。

【００４３】

同様に他のトラックについて、同様の項目が読み出される。これらの読み出された項目からオフセットの順序でチャンク毎のオフセット及びサンプル毎のオフセットが記述されたテーブルが作成される。

【００４４】
即ち、図１０に示すようにオーディオトラックに属するオーディオチャンク（Ａ　ｃｈｕｎｋ）及びビデオトラックに属するビデオチャンク（Ｖ　ｃｈｕｎｋ）が交互に表れるようなメディアデータボックス１３に格納されているメディアデータでは、オフセット０からオフセットｘで示されるチャンクに関するテーブルが作成され、各チャンクに関するオフセットアドレスがｃｈｕｎｋ＿ｏｆｆｓｅｔからそのテーブルにコピーされる。また、そのテーブルには、各チャンクを構成するサンプル数に応じてサンプルの項目が作成され、該当するサンプルのサンプルサイズからそのサンプルの位置及びそのサイズが記述される。作成されたテーブルにおいて、チャンクの総数及びサンプルの総数は、各トラックのチャンク数及びサンプル数でその総数が確認される。

【００４５】
次に、このテーブルが参照されてステップＳ１３に示すようにメディアデータボックス１３内の最初のサンプルが暗号化されてローカルメモリ１０６に書き込まれる。次に、暗号化されたサンプルの番号Ｎがステップ Ｓ１３においてメディアデータボックス１３内の最後のサンプルかが確認される。暗号化されたサンプルが最後のサンプルでない場合には、ステップＳ１４に示されるように暗号化されるべきサンプル番号が１つ増加され、再びステップＳ１２に示すようにテーブルからサンプルの位置及びサイズを取得するステップに戻され、ステップＳ１３において、その該当サンプルが暗号化される。ステップＳ１２からステップＳ１５が繰り返されてステップＳ１５において暗号化されたサンプルがメディアデータボックス（ｍｄａｔ）１３内の最後のサンプルに相当する場合には、その処理がステップＳ１８に示すように終了される。

【００４６】
メディアデータボックス（ｍｄａｔ）１３以外の他のボックスが暗号化される場合には、図１３に示すように図１２と同様にステップＳ１１からステップＳ１５が実行される。ステップＳ１５において暗号化されたサンプルがメディアデータボックス（ｍｄａｔ）１３内の最後のサンプルに相当する場合には、メディアデータボックス１３内の実データの暗号化が終了されたとして他のボックスがステップＳ１６で暗号化される。例えば、メディアデータボックス１３内の実データの暗号化するために利用されたムービーボックス１２（ｍｏｏｖ）が暗号化される。当然ながら、既に説明したようにメディアデータボックス１３及びムービーボックス１２（ｍｏｏｖ）内のサイズ・フィールド、タイプ・フィールド、更には、ラージサイズ・フィールドは、何れも暗号化されない。

【００４７】
ステップＳ１７において、全てのボックスが暗号化されていない場合には、再びステップＳ１６に戻されて次々にＭＰ４ファイル内のボックスが暗号化される。

【００４８】
ステップＳ１７において、全てのボックスの暗号化が終了すると、その処理がステップＳ１８に示すように終了される。

【００４９】
上述した説明において、メディアデータボックス１３では、既に説明したようにサンプルが所定のブロック長毎に暗号化され、残余の部分が生じた場合には、その部分は暗号化されないこととなる。例えば、所定のブロック長が８バイトであり、サンプルがこの８バイトの整数（ｎ）倍のサイズＮバイト（Ｎ＝ｎ×８）を有する場合には、図１４に示すようにそのサンプルは、非暗号化の残余なしで暗号化される。これに対して、所定のブロック長が８バイトであり、サンプルがこの８バイトの整数（ｎ）倍のサイズを超えるバイト（Ｎ＝ｎ×８＋ｍ、但し、ｍ＜８）を有する場合には、図１５に示すようにそのサンプルの所定のブロック長部分８バイトの整数倍の部分（ｎ×８ビット）は、暗号化され、残余の部分（ｍバイト）は、暗号化されない。同様に、所定のブロック長が８バイトであり、サンプルがこの８バイトの整数（ｎ）倍のサイズ以内のバイト（Ｎ＜８）を有する場合には、図１６に示すようにそのサンプルは、暗号化されないこととなる。

【００５０】

尚、図１３を参照して説明した暗号化処理では、前提として、ローカルメモリ１０６上にＭＰ４ファイルが蓄積されていることを想定しているが、即ち、ファイルの生成は、完了しているものとしている。しかしながら、ファイルが生成されながらの暗号化処理が実施されても良いことは明らかである。

【００５１】

この暗号化された音声及び映像データを含むファイルは、一例として図１７に示すような動画像再生システム１００で復号化される。この動画像記録システム１００における復号化は、図１８に示すような手順で実現される。この動画像記録システム１００における復号化の手順についてこの図１７及び図１８を参照して説明する。

【００５２】

図１７は、ＭＰ４ファイルの暗号化された音声及び映像データを復号化して音声及び映像信号に変換する動画像再生システム２００を示している。この動画像再生システム２００においては、図１３に示した暗号化処理が施されたＭＰ４ファイルがローカルメモリ２０６に入力され、このローカルメモリ２０６に格納される。図１８を参照して説明するように暗号化されたファイルは、暗号復号化部２０７にて所定の暗号復号方法で暗号が復号され、再度、ローカルメモリ２０６に配置される。このローカルメモリに展開されたファイルがファイル解析部２０５において音声符号化ストリーム及びビデオ符号化ストリームに分離され、それぞれオーディオデコーダ２０２及びビデオデコーダ２０４に供給される。オーディオデコーダ２０２は、供給された音声符号化ストリームをデコードして音声信号をスピーカ２０１に出力して再生させている。また、ビデオデコーダ２０４は、供給されたビデオ符号化ストリームをデコードしてビデオ信号を画像出力装置２０３に出力し、動画像を画像出力装置２０３に表示させている。

【００５３】

図１８を参照して暗号化されファイルを復号する為の手順を説明する。ここでは、前提として、ローカルメモリ２０６上には、暗号化されたＭＰ４ファイルが蓄積され、また、メディアデータボックス１３内では、サンプル毎に暗号化されているものとする。

【００５４】

暗号の復号化処理が開始されると（ステップＳ２０）、メディアデータボックス（ｍｄａｔ）１３を除く他のボックスについて、ステップＳ２１に示すように暗号の復号化処理が実施される。図４から図７を参照して既に説明したように各ボックスにおいては、サイズ・フィールド、タイプ・フィールド、更には、ラージサイズ・フィールドは、何れも暗号化されていないことから、これらのフィールドが参照されてメディアデータボックス（ｍｄａｔ）１３以外のボックスかが確認され、各ボックスの暗号化されたボックスデータ部が復号化される。復号化されたボックスは、再びローカルメモリ２０６上に蓄積される。ステップＳ２２に示すようにメディアデータボックス（ｍｄａｔ）１３以外のボックスの復号化処理が終了するまで繰り返され、この処理が終了すると、ステップＳ２３で示す次の処理へ移行される。

【００５５】

メディアデータボックス（ｍｄａｔ）１３のみが暗号化され、他のボックスが暗号化されていない場合には、スタートＳ２０後ステップＳ２３に示す処理が実施される。

【００５６】

ステップＳ２３においては、復号化処理が施されたムービーボックス１２がファイル中から検索される。ムービーボックス１２が検索されると、ステップＳ２４に示すように暗号化時と同様の方法でムービーボックス１２中に格納されているトラック毎のチャンクオフセットボックス（ｓｔｃｏ）及びサンプルトゥチャンクボックス（ｓｔｓｃ）、サンプルサイズボックス（ｓｔｓｚ）が検索され、それらに保持されているテーブルがメモリ上に保持される。即ち、ステップＳ１２において、Ｎの初期値は１に設定され、このムービーボックス１２内の最初のトラックｔｒａｋ内に記述された最初のチャンクのチャンクオフセットｓｔｃｏが読み出され、このチャンクオフセットｓｔｃｏ内のｃｈｕｎｋ＿ｏｆｆｓｅｔからそのオフセットアドレスが読み出されると共にサンプルサイズボックスｓｔｓ

ｚのｅｎｔｒｙ＿ｓｉｚｅからそのトラックに属する全てのサンプルサイズが読み出される。また、チャンクオフセットｓｔｃｏ内のｅｎｔｒｙ＿ｃｏｕｎｔからそのトラック内の全てのチャンク数が読み出され、また、チャンクボックスに対するサンプルを意味するｓｔｓｃのｓａｍｐｌｅ＿ｐｅｒ＿ｃｈｕｎｋから各チャンクのサンプル数が読み出され、サンプルサイズボックスｓｔｓｚのｓａｍｐｌｅ＿ｃｏｕｎｔからそのトラック内の全てのサンプル総数が読み出される。

【００５７】

同様に他のトラックについて、同様の項目が読み出される。これらの読み出された項目からオフセットの順序でチャンク毎のオフセット及びサンプル毎のオフセットが記述されたテーブルが作成される。

【００５８】

即ち、図１０に示すようにオーディオトラックに属するオーディオチャンク（Ａ　ｃｈｕｎｋ）及びビデオトラックに属するビデオチャンク（Ｖ　ｃｈｕｎｋ）が交互に表れるようなメディアデータボックス１３に格納されているメディアデータでは、オフセット０からオフセットｘで示されるチャンクに関するテーブルが作成され、各チャンクに関するオフセットアドレスがｃｈｕｎｋ＿ｏｆｆｓｅｔからそのテーブルにコピーされる。また、そのテーブルには、各チャンクを構成するサンプル数に応じてサンプルの項目が作成され、該当するサンプルのサンプルサイズからそのサンプルの位置及びそのサイズが記述される。作成されたテーブルにおいて、チャンクの総数及びサンプルの総数は、各トラックのチャンク数及びサンプル数でその総数が確認される。

【００５９】

次に、このテーブルが参照されてステップＳ２５に示すように最初のサンプルが復号化されてローカルメモリ１０６に書き込まれる。次に、復号化されたサンプルの番号Ｎがステップ１３においてメディアデータボックス１３内の最後のサンプルかが確認される。復号化されたサンプルが最後のサンプルでない場合には、ステップＳ２７に示されるように復号化されるべきサンプル番号が１つ増加され、再びステップＳ２４に示すようにテーブルからサンプルの位置及びサイズを取得するステップに戻され、ステップＳ２５において、その該当サンプルが復号化される。ステップＳ２４からステップＳ２７が繰り返されて暗号化されたサンプルがメディアデータボックス（ｍｄａｔ）１３内の最後のサンプルに相当する場合には、メディアデータボックス１３内の実データの復号化が終了される。

【００６０】

上述した実施例の変形例として、ムービーフラグメントボックスを参照して各サンプルのオフセットを獲得しても良い。即ち、ムービーフラグメントボックスがあるＭＰ４ファイルでは、ムービーフラグメントボックスにチャンクオフセットｓｔｃｏ及びサンプルサイズｓｔｓｚが記述されている。従って、このチャンクオフセットｓｔｃｏ及びサンプルサイズｓｔｓｚを解析することによって同様に各サンプルのオフセットを獲得することができる。

【００６１】

上述した実施例においては、このサンプルのオフセット値及びサイズを用いてサンプル内のデータが暗号化されている。サンプルは、符号化ストリームのデコードに必要な最小の単位のため、サンプル単位にアクセスすることができれば、前述の特殊再生において、任意の位置のサンプルを効率的にアクセスすることが可能となる。即ち、図１３に示す処理において、ステップＳ１０からステップＳ１２が実施され、ステップＳ１２において、Ｎ番目のサンプルが目的とされるサンプルであれば、その目的とされるサンプルのみが復号化され、この復号化されたサンプルが音声或いは映像信号にデコードされて再生される。この目的とされるサンプルのみの再生によって、動画の再生においては、例えば、早送り再生、巻き戻し再生、ランダムアクセス再生、ユーザが再生停止したところから、再度再生を再開するレジューム再生が実現される。音声の再生においても同様に再生可能となる。

【００６２】

尚、上述した実施例においては、メディアデータボックス１３内では、サンプル毎に暗号化されている。このサンプル毎の暗号化に代えて、チャンク毎にチャンク内のデータが暗号化されても良い。既に説明したように、チャンクは、メディアデータ内の同一メディアのサンプルが連続している時の集合を示している。上記のサンプル単位毎に暗号化を行う場合と同様にチャンク毎に暗号化されれば良い。このチャンク毎の暗号化では、サンプル毎の暗号化に比べて、暗号化のリセットの回数が削減されるため、暗号化及び暗号を解く処理を軽減することが可能となる。尚、チャンク毎の暗号化及び復号化については、図１３及び図１８において、収集されるチャンクの情報を処理することによってサンプルと同様にチャンクの暗号化及び復号化が可能となる。

【００６３】

この発明の暗号化方法及び復号化方法は、ＭＰ４ファイル・フォーマットを格納する機器、例えば、携帯電話、デジタルカメラ、デジタルムービー、デジタルハードディスクレコーダー、ＰＤＡ等に適用することができる。

【００６４】

また、同様のボックス構造を用いているＪＰＥＧ２０００のファイル・フォーマットにあっても、この発明の暗号化方法及び復号化方法を適用することができる。

【００６５】

以上のように、この発明の実施例によれば、ボックス毎に暗号化を行うことによって、ＭＰ４データ内に存在する任意のボックスに効率的にアクセスすることが可能となる。さらに、サイズ・フィールド、タイプ・フィールド以外を暗号化することにより、平文であるサイズ・フィールド、タイプ・フィールドを用いて暗号を解く処理を行わずに所望のボックスへアクセスすることができる。

【００６６】

また、この発明の実施例によれば、音声或いは動画の符号化データを含むボックスにアクセスすることができ、また、そのボックス内のサンプル或いはチャンクに効率的にアクセスすることができ、音声或いは動画の特殊再生が実現することが可能となる。

【００６７】

【発明の効果】

以上のように、この発明によれば、コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法が提供される。

【図面の簡単な説明】

【図１】図１は、この発明の一実施例に係る暗号化方法が適用されるＭＰ４ファイルの構造を概略的に示す平面図である。

【図２】図１に示される各ボックスの一般的な構造を概略的に示す平面図である。

【図３】図２に示した構造とは異なる他のタイプに係るボックスの構造を概略的に示す平面図である。

【図４】図１に示されるメディアデータボックス以外の他のトップレベルボックスに対する暗号化を説明する為の平面図である。

【図５】図２に示した構造とは異なる他のタイプに係るメディアデータボックス以外の他のトップレベルボックスに対する暗号化を説明する為の平面図である。

【図６】図４に示されるボックスに対する暗号化においてブロック単位で暗号化を施し、残余のデータが生じた際にその残余データに対しては暗号化を施さないことを説明する為の平面図である。

【図７】図１に示されるメディアデータボックスのヘッダの構造及びその非暗号化を示す平面図である。

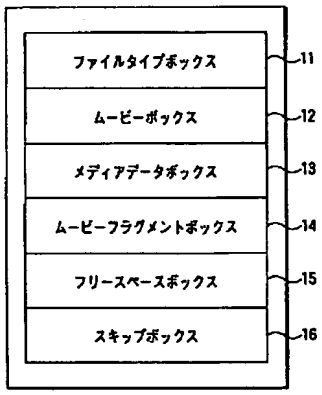
【図８】図１に示されるムービーボックスの構造を示す平面図である。

【図９】（ａ）及び（ｂ）は、図１に示されるムービーボックスの他の構造を示す平面図である。

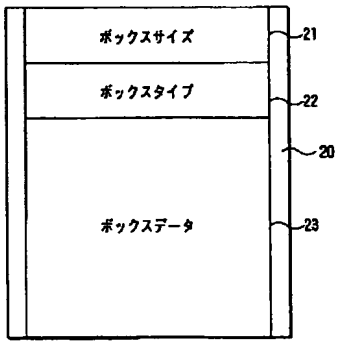
【図１０】図１に示されるメディアデータボックス内のデータ構造を説明する為の平面図

である。
【図１１】この発明の一実施例に係る暗号化システムを概略的に示すブロック図である。
【図１２】図１１に示される暗号化システムにおける暗号化方法を説明する為のフローチャートである。
【図１３】図１１に示される暗号化システムにおける他の暗号化方法を説明する為のフローチャートである。
【図１４】図１４は、図１に示されたメディアデータボックスを暗号化した際の一例を示す平面図である。
【図１５】図１に示されたメディアデータボックスを暗号化した際の他の例を示す平面図である。
【図１６】図１に示されたメディアデータボックスを暗号化した際の更に他の例を示す平面図である。
【図１７】この発明の一実施例に係る暗号復号化システムを概略的に示すブロック図である。
【図１８】図１７に示される暗号復号化システムにおける暗号復号化方法を説明する為のフローチャートである。
【符号の説明】
１１．．．ファイルタイプボックス
１２．．．ムービーボックス
１３．．．メディアデータボックス
１４．．．ムービーフラグメントボックス
１５．．．フリースペースボックス
１６．．．スキップボックス
２０．．．ボックス
２１．．．サイズ・フィールド
２２．．．タイプ・フィールド
２３．．．ボックスデータ部
１０２．．．オーディオエンコーダ
１０４．．．ビデオエンコーダ
１０５．．．ファイル生成部
１０６．．．ローカルメモリ
１０７．．．暗号化部１０７
２０２．．．オーディオデコーダ
２０４．．．ビデオデコーダ
２０５．．．ファイル解析部
２０６．．．ローカルメモリ
２０７．．．暗号復号化部

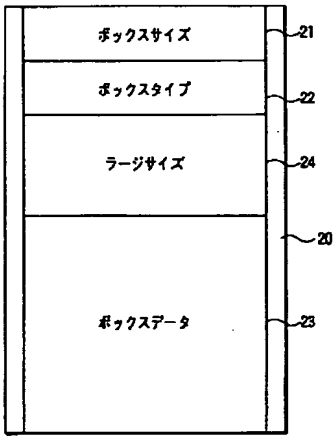
【図１】


ファイルタイプボックス
ムービーボックス
メディアデータボックス
ムービーフラグメントボックス
フリースペースボックス
スキップボックス
11
12
13
14
15
16

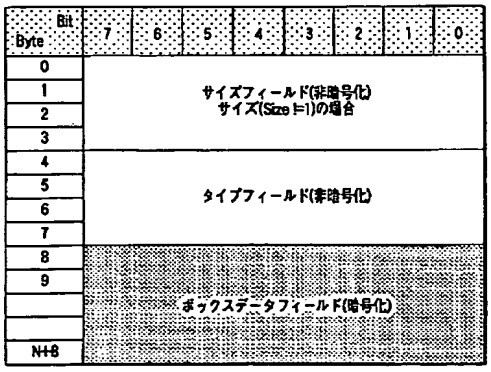
【図２】


ボックスサイズ
ボックスタイプ
ボックスデータ
21
22
20
23

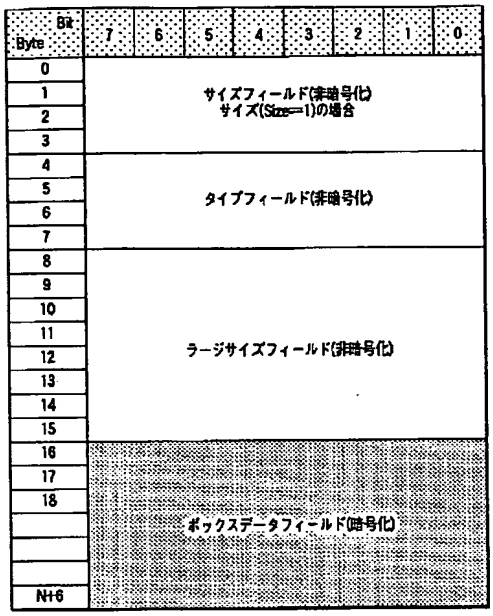
【図３】


ボックスサイズ
ボックスタイプ
ラージサイズ
ボックスデータ
21
22
24
20
23

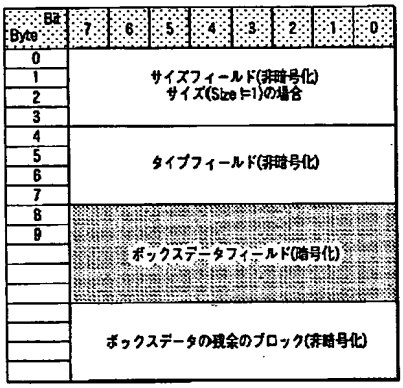
【図４】


Bit
Byte
7
6
5
4
3
2
1
0
0
1
2
3
4
5
6
7
8
9
N-8
サイズフィールド(非暗号化)
サイズ(Size != 1)の場合
タイプフィールド(非暗号化)
ボックスデータフィールド(暗号化)

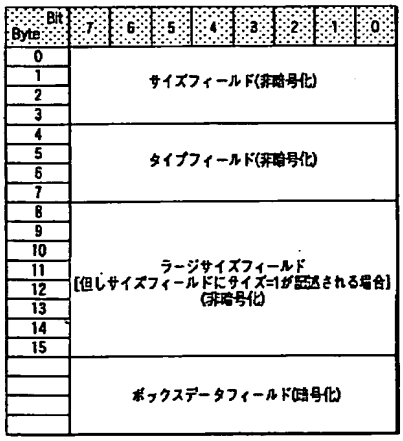
【図５】


Bit
Byte
7 6 5 4 3 2 1 0
0
1
2
3
サイズフィールド(非暗号化)
サイズ(Size==1)の場合
4
5
6
7
タイプフィールド(非暗号化)
8
9
10
11
12
13
14
15
ラージサイズフィールド(非暗号化)
16
17
18
ボックスデータフィールド(暗号化)
N+6

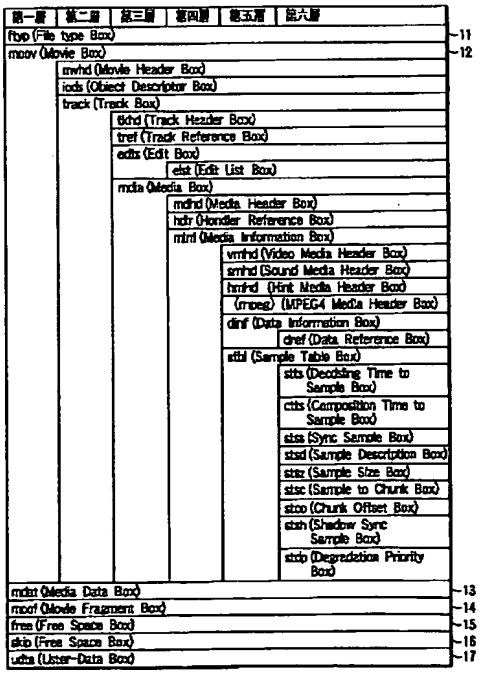
【図６】


Bit
Byte
7 6 5 4 3 2 1 0
0
1
2
3
サイズフィールド(非暗号化)
サイズ(Size!=1)の場合
4
5
6
7
タイプフィールド(非暗号化)
8
9
ボックスデータフィールド(暗号化)
ボックスデータの残余のブロック(非暗号化)

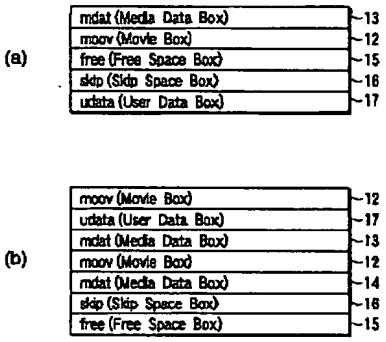
【図７】


Bit
Byte
7 6 5 4 3 2 1 0
0
1
2
3
サイズフィールド(非暗号化)
4
5
6
7
タイプフィールド(非暗号化)
8
9
10
11
12
13
14
15
ラージサイズフィールド
(但しサイズフィールドにサイズ=1が記述される場合)
(非暗号化)
ボックスデータフィールド(暗号化)

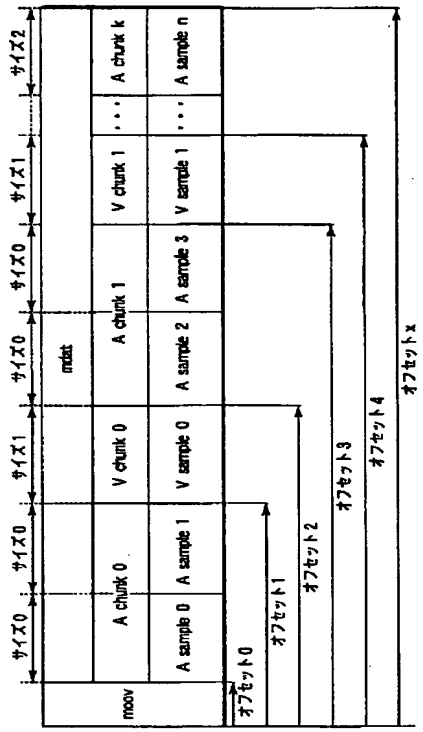
【図８】


第一層
第二層
第三層
第四層
第五層
第六層
ftyp (File type Box)
11
moov (Movie Box)
12
mvhd (Movie Header Box)
iods (Object Descriptor Box)
track (Track Box)
tkhd (Track Header Box)
tref (Track Reference Box)
edts (Edit Box)
elst (Edit List Box)
mdia (Media Box)
mdhd (Media Header Box)
hdlr (Handler Reference Box)
minf (Media Information Box)
vmhd (Video Media Header Box)
smhd (Sound Media Header Box)
hmhd (Hint Media Header Box)
(mpeg) (MPEG4 Media Header Box)
dinf (Data Information Box)
dref (Data Reference Box)
stbl (Sample Table Box)
stts (Decoding Time to Sample Box)
ctts (Composition Time to Sample Box)
stss (Sync Sample Box)
stsd (Sample Description Box)
stsz (Sample Size Box)
stsc (Sample to Chunk Box)
stco (Chunk Offset Box)
stsh (Shadow Sync Sample Box)
stdp (Degradation Priority Box)
mdat (Media Data Box)
13
moof (Movie Fragment Box)
14
free (Free Space Box)
15
skip (Free Space Box)
16
udta (User-Data Box)
17

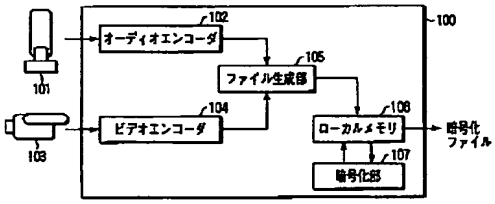
【図９】



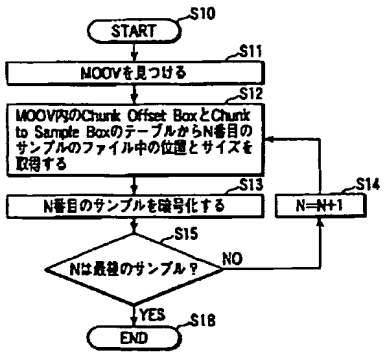
【図１０】



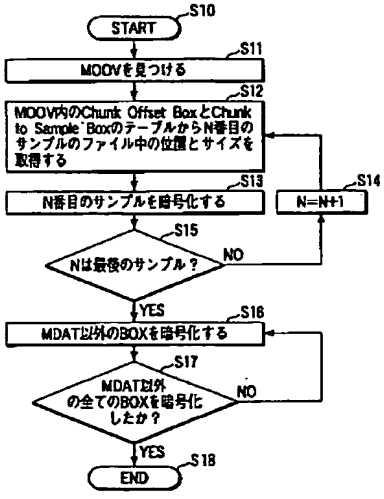
【図１１】



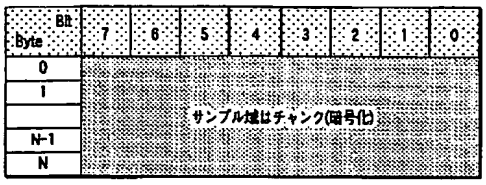
【図１２】



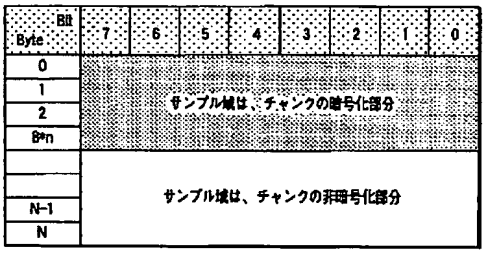
【図１３】



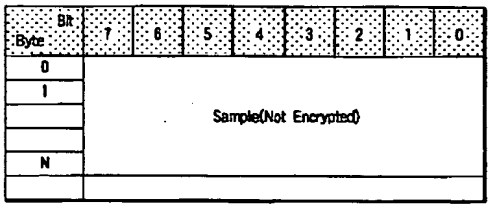
【図１４】



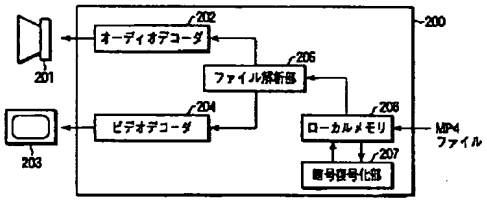
【図１５】



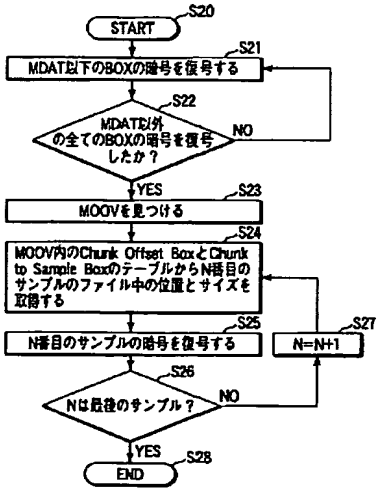
【図１６】



【図１７】



【図１８】



フロントページの続き

(72)発明者 佐藤 順
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内
(72)発明者 寺内 亨
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内

Ｆターム(参考) 5B017 AA03 BA07 CA16
5C053 FA13 GB37 HA21
5J104 AA12 AA33 CA02 DA04 NA02 NA27 PA14